What Is Claimed Is:

1. A method of producing at least one alert indication based on a number of events derived from an enterprise comprising:

providing a plurality of enterprise device outputs, at least a portion of the outputs having different formats, each output containing an event relating to an enterprise device;

translating each output into a common format event,

adding knowledge to the common format event using knowledge base table files to generate a knowledge-containing common format event; and

applying one or more rules from a set of rules to the knowledge-containing common format event to generate the alert indication.

2. The method of claim 1, wherein the common format event contains at least a generic description of a specific event occurring as part of each device output.

3. The method of claim 1, wherein generating the knowledge-containing common format event further comprises comparing the common format event for each network device to a number of knowledge base table entries contained in a knowledge base table, wherein knowledge is added from one or more of the knowledge base table entries when a match between the translated

common format event and the entry in the knowledge base table is made.

4. The method of claim 1, wherein the enterprise devices are selected from the group consisting of a server, a firewall, a modem, a work station, a router, a remote machine, an intrusion detection system, an identification and authentication server, network monitoring and management systems, network components, and one or more combinations thereof.

5. The method of claim 1, wherein the translating step further comprises:

matching data values in the device output with a signature specification for each enterprise device, the signature specification containing:

a number of signatures;

a first location identifier for each signature; and

a first key;

wherein the signature is a listing of names found in the device output, the first location identifier determines the method used to locate the name in the device output, and the first key determines where to locate the name in the device output;

identifying a message type from a plurality message types for each enterprise device based on the device output as part of the translated common format event;

producing the remainder of the translated common format event in argument name and argument value pairs using an argument specification, the argument specification containing;

a listing of arguments;

a field type;

a second location identifier for each argument; and

a second key;

wherein each argument is a listing of argument names for inclusion in the translated common format event, the field type specifies the form of an argument value found in the device output, the second location identifier determines the location of each argument value, and the second key locates the argument value in the device output to be displayed with the argument name.

6. The method of claim 1, wherein the knowledge-containing common format event comprises one or more names selected from the group of a device alert, a generic alert, a threat severity, a benign explanation, a recommended action, a common vulnerabilities and exposure code, a conclusion, and a category code, and a corresponding value for each name.

7. The method of claim 1, wherein one or more rules determine when or whether the knowledge-containing common format event is generated, and final rule-based additions content of such generated events.

8. The method of claim 7, wherein the rule requires that the each output occur a number of times over a period of time before an alert indication is generated.

9. The method of claim 1, wherein the output is one of an unauthorized login, an unauthorized physical entry, and an attempt to bypass a firewall.

10. The method of claim 3, wherein the translating step further comprises:

matching data values in the device output with a signature specification for each enterprise device, the signature specification containing:

a number of signatures;

a first location identifier for each signature; and

a first key;

wherein the signature is a listing of names found in the device output, the first location identifier determines the method used to locate the name in the device output, and the first key determines where to locate the name in the device output;

identifying a message type from a plurality message types for each enterprise device based on the device output as part of the translated common format event;

producing the remainder of the translated common format event in argument name and argument value pairs using an argument specification, the argument specification containing;

a listing of arguments;

a field type;

a second location identifier; and

a second key;

wherein each argument is a listing of argument names for inclusion in the translated common format event, the field type specifies the form of an argument value found in the device output, the second location identifier determines the location of each argument value, and the second key locates the argument value in the device output to be displayed with the argument name.

11. The method of claim 10, wherein the rule determines when or whether the knowledge-containing common format event is generated.

12. The method of claim 11, wherein the rule requires that each output occur a number of times over a period of time before an alert indication is generated.

13. The method of claim 1, wherein the alert indication includes at least a text message describing the event contained in the output of the enterprise device.

14. The method of claim 13, wherein a threat level is included as part of the alert indication.

15. A system for producing at least one alert indication based on a number of events derived from an enterprise comprising:

a plurality of enterprise devices, each device capable of producing an output;

a number of translation files, the translation files allowing the output to be translated into a common format event;

a number of knowledge base table files, matching of the common format event with one or more of the knowledge base table files adding knowledge from the matched file to generate a knowledge-containing common format event;

a number of rule files, the rule files governing generation of the alert indication.

16. The system of claim 15, wherein the enterprise devices are selected from the group consisting of a server, a firewall, a modem, a work station, a router, a remote machine, an intrusion detection system, an identification and authentication server, network monitoring and management systems, network components, and one or more combinations thereof, or any generator of data streams on the computer network.

17. The system of claim 15, wherein the knowledge-containing common format event comprises one or more names selected from the group of a device alert, a generic alert, a threat severity, a benign explanation, a recommended action, a CVE, a conclusion, and a category code, and a corresponding value for each name.

18. The system of claim 15, wherein the common format event comprises a message, and a number of name and value pairs derived from the output of the enterprise device.

19. The system of claim 17, wherein the rule files govern at least the frequency of the generation of the alert indication.

20. The system of claim 19, wherein the common format event comprises a message, and a number of name and value pairs derived from the output of the enterprise device.

21. The method of claim 7, wherein the rule adds information to the knowledge-containing common format event.

22. The system of claim 11, wherein the rule adds information to the knowledge-containing common format event.